

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION**

TRINITY SOBER LIVING, LLC,)	
)	
Plaintiff,)	
)	Case No. 1:19-cv-07321
v.)	
)	Judge Robert W. Gettleman
VILLAGE OF HINSDALE, ILLINOIS,)	
)	
Defendant.)	
)	
UNITED STATES OF AMERICA,)	
)	
Plaintiff,)	
)	Case No. 1:20-cv-06959
v.)	
)	Judge Robert W. Gettleman
VILLAGE OF HINSDALE, ILLINOIS,)	
)	
Defendant.)	

**STIPULATION AND ORDER REGARDING DISCOVERY OF
ELECTRONICALLY-STORED INFORMATION AND OTHER DOCUMENTS**

Pursuant to Rule 26(f) of the Federal Rules of Civil Procedure, Plaintiffs, Trinity Sober Living LLC and the United States of America (collectively, “Plaintiffs”), and Defendant Village of Hinsdale (each a “Party” and collectively, the “Parties”) have entered into this Stipulation to reduce the time, expense, and other burdens of discovery of electronically stored information (“ESI”) and hereby incorporate the terms of this stipulation into the proposed Case Management Order submitted to the Court.

I. PRESERVATION OF ESI

1. The parties agree to preserve all ESI for purposes of this litigation. By agreeing to preserve such ESI, the parties do not concede that such ESI is discoverable, nor are they waiving any claim of privilege.

2. This Stipulation does not modify any party's obligation to maintain or preserve ESI where otherwise required by law, pursuant to a court or administrative order, or in response to other anticipated litigation.

II. LIMITATIONS ON OBLIGATION TO PRESERVE AND PRODUCE ESI

3. Notwithstanding the above section, the parties agree that they do not need to take specific, affirmative steps to preserve, for purposes of this litigation, the following categories of ESI:

- a. Delivery or read receipts of e-mail;
- b. Logs or other data from video conferencing (including, *e.g.*, Skype or Zoom) or instant messaging tools involving (i) attorneys for Plaintiffs (and their staff) and/or (ii) attorneys for defendants (and their staff);
- c. Temporary or cache files, including internet history, web browser cache, and cookie files, wherever located;
- d. Internally facing server system logs;
- e. Externally facing or hosted file sharing systems;
- f. System data from photocopiers or fax machines;
- g. Auto-saved copies of electronic documents;
- h. Deleted, slack, fragmented, or other data only accessible by forensics;

i. Random Access Memory, temporary files, or other ephemeral data that are difficult to preserve without disabling the operating system;

j. Logs of other data from audio calls (including, *e.g.*, landline phones, mobile devices, and Voice Over Internet Protocol) made to or from (i) attorneys for the United States (and their staff) and/or (ii) attorneys for defendants (and their staff); and

k. Voicemail messages on the voicemail systems of (i) attorneys for Plaintiffs (and their staff) and/or (ii) attorneys for defendants (and their staff).

4. When duplicate copies¹ of relevant ESI exist in more than one location, the parties need not preserve all duplicates, as follows:

a. ESI that exists or is stored on mobile or portable devices (*e.g.*, smartphones, tablets, thumb drives, CDs, or DVDs) or file sharing sites need not be preserved, *provided that* duplicate copies of the ESI, including metadata, are preserved in another location that is reasonably accessible to the party.

b. ESI that exists or is stored on backup tapes, continuity of operations or disaster recovery systems, data or system mirrors or shadows, and other systems that are used primarily for the purpose of system recovery or information restoration and are not reasonably accessible (“Backup Systems”) need not be preserved, *provided that* duplicate copies of the ESI, including metadata, are preserved in another location that is reasonably accessible to the party. However, if a party knows that relevant ESI exists only on a party’s Backup Systems, the party will take reasonable steps to preserve ESI on the

¹ “Duplicates,” in the context of ESI, are copies of identical documents identified with matching MD-5 hashes, which is a mathematically-calculated 128 bit value used to create a unique identifier for an electronic file. *See In re Actos (Pioglitazone) Prods. Liability Litig.*, MDL No. 6:11-md-2299, 2012 WL 7861249, at *10-11 (W.D. La. July 27, 2012) (“All files bearing an identical MD5 hash value are a duplicate group.”).

Backup System until the parties can agree on how and when the ESI will be preserved or produced. If the parties cannot reach agreement, they will seek a ruling from the Court.

5. The parties need not take specific, affirmative steps to preserve, for purposes of this litigation, relevant documents, things, or ESI (including internal communications, draft versions, and collaboration on case-related work) created by and/or exchanged solely between and among: (1) attorneys for the Plaintiffs (and their staff); and (2) attorneys for defendants (and their staff).

6. The parties agree not to seek discovery of documents, things, and ESI that they have agreed not to preserve pursuant to this section. The parties do not need to list these items on a privilege log prepared and served in connection with discovery in this case.

III. IDENTIFICATION & PRODUCTION OF ESI AND OTHER DOCUMENTS

7. ESI and hard copy documents must be produced on CD, DVD, thumb drive, or hard drive, or by file-transfer protocol (FTP) link, as specified herein.

8. **TIFFs:**

a. With the exception of MS Access files; MS Excel files, or any other type of spreadsheet or comma-separated-value files; media files; or other formats where imaging is impracticable, Bates-stamped images will be produced as single page Group IV TIFFs of at least 300 dpi resolution.

b. Each image will use the Bates number of the first page of the document as its unique file name.

c. Images may be black-and-white or color. However, to the extent the black-and-white format obscures or degrades information (*e.g.* color-coded graphs or

charts, printed photographs, or redlines) as to a particular document, the producing party must produce a color image.

d. If a document qualifies for confidential treatment pursuant to the terms of a protective order entered by the Court, the designation shall be shown on the face of all TIFFs produced for the document.

e. For all files produced in native format without imaging, a single Bates-stamped placeholder TIFF image shall be produced, with language on the page noting the production of the document solely in native format.

f. All productions will include a delimited data file or “load file” that references each TIFF in the corresponding production.

9. **Text Files:** Each produced document shall be accompanied by a text file as set out below. All text files shall be provided as a single document level text file for each item, not one text file per page. Each text file shall be named to use the Bates number of the first page of the corresponding production item.

a. **OCR:** Scanned paper documents will be accompanied by an OCR text file. The parties will endeavor to generate accurate OCR and will utilize quality OCR processes and technology. The parties acknowledge, however, that due to poor quality of the originals, not all documents lend themselves to the generation of accurate OCR. OCR text files should indicate page breaks where possible.

b. **ESI:** Emails and other ESI will be accompanied by extracted text taken from the electronic file itself.

c. **Redacted documents:** Any ESI document produced in redacted form shall be accompanied by an OCR text file, not extracted text.

10. **Native Format:**

a. A copy of any MS Excel, or any other type of spreadsheet or comma-separated-value file shall be produced in native format (meaning in the same overall electronic format as it is kept in the ordinary course of business).

b. Audio files and video files shall be produced in native format, unless that is a proprietary format, in which case the file(s) shall be converted into a non-proprietary format such as .MP4.

c. The parties agree to meet and confer in any instance where the receiving party contends that native format production is necessary with respect to any particular document that has been produced in TIFF format.

d. For each file produced in native format, a unique document number shall be used as the file name, with the original file name and file extension preserved in the corresponding data file described in the following paragraph 11.

e. Excel or other types of spreadsheets shall be produced with all cells unlocked.

11. **Metadata:** ESI must be collected and prepared for production in a way that preserves existing metadata to the extent reasonably possible. A data file in .dat format (or other format agreeable to the receiving party) containing file-level original metadata and production metadata must accompany each production. Each file produced will have a corresponding record (row) in the data file. The included metadata fields shall be those listed in Appendix A hereto, wherever available and applicable.

12. If a document has been prepared in several copies, or additional copies have been made that are not identical (or are no longer identical by reason of subsequent notation or other modification of any kind whatsoever), each non-identical copy is a separate document.

13. **Deduplication:**

a. Deduplication will be used to remove exact duplicate documents from the production. The Parties agree to use MD-5 hash values for deduplication and calculate those values for all ESI at the time of collection or processing.

b. With respect to e-mails and attachments, de-duplication shall be used solely at the parent e-mail level, such that a document is produced once for every single time it is attached to any produced e-mail, even though one or more produced copies of that attachment might be exact duplicates of each other.

c. Notwithstanding sub-paragraph (a) above, a producing party is permitted to globally deduplicate e-mail such that only one custodian's copy is produced for each e-mail with unique content (regardless of MD-5 hash value), but only if accurate and complete "Duplicate Custodian" metadata is produced in the production data file (under paragraph 11 above) to indicate all custodians with a copy of the e-mail in question.

14. **Use of Search Criteria to Identify ESI:** It is the responsibility of the Party responding to a discovery request to identify and produce responsive information, including ESI. The Parties agree to meet and confer if either believes that the use of keyword search criteria or analytic tools should be used to identify responsive ESI.

15. With respect to email, the parties agree to produce a single copy of all responsive, non-privileged emails in each thread or chain and will not restrict production to the most

inclusive emails. Any e-mail attachment(s) shall be produced so as to sequentially follow the parent email in Bates order.

16. PowerPoint files and Word documents shall be produced such that any track changes, comments and speaker notes that were visible in the original document are visible in the production TIFFs and extracted text.

17. Text messages or social media content (including comments, “likes,” sharing, and other interactions with the post(s)) shall be produced as images, including information about the participants and the date/time of the communications. Neither this provision nor any other herein constitutes an admission by any party that a search of any particular source or file type is reasonable, proportional to the needs of the case, or likely to lead to the discovery of relevant evidence.

18. For production of tangible things and production of information from a structured database, proprietary software, vendor-managed software, or other source from which neither native production nor TIFF imaging is reasonably practicable, the parties will meet and confer before making any production to attempt to agree on a reasonable and proportional form of production that maintains the integrity of the documents or tangible things.

19. Oversized documents (*e.g.*, architectural, engineering, or zoning plans) must be produced as JPEG images or in hard copy paper form so as to retain the resolution and scale of the original document.

20. ESI and (scanned) hard copy paper documents must be produced on media or through an FTP method appropriate to the data size. Production media or a communication with a production FTP link will be clearly labeled to indicate: (1) the Party producing the documents; (2) the date of the production; and (3) the Bates range. The United States may

utilize the Justice Electronic File Sharing (“JEFS”) system for its productions in lieu of an FTP method.

21. If a party needs to redact a portion of a document that is of a type to be produced in native format, the parties will meet and confer regarding production of the redacted document.

22. The parties agree to remove all encryption or password protection for all ESI produced, where practicable. Where removal is not practicable, the parties agree to provide passwords or assistance needed to open encrypted files, wherever information in the producing party’s possession allows.

IV. PRIVILEGED DOCUMENTS & ESI

23. If any discovery request appears to call for the production of documents, things or ESI covered by Section II, *supra*, the responding party is not required to produce or identify such information on a privilege log. However, if a party preserves relevant documents, things, or ESI covered by Section II in order to support a claim or defense in this case, the Party shall produce such information or identify it on a privilege log notwithstanding this section.

24. The Parties agree that a disclosure of information contained within documents, things, and ESI that is protected by attorney-client privilege, work product protection, and/or applicable governmental privileges (such as deliberative process):

- a. does not operate as a subject matter waiver if the disclosure is inadvertent;
and
- b. does not operate as a waiver as to disclosed information if: 1) the disclosure is inadvertent; 2) the holder of the privilege or protection took reasonable steps

to prevent disclosure; and 3) the holder promptly took reasonable steps to rectify the error.

25. If the producing Party inadvertently discloses information that it asserts is privileged or protected, it will notify the receiving party within seven (7) days of discovery of the disclosure and provide the production date, number, and volume of the disc, drive, or FTP or JEFS delivery in which the information was produced (“production media”), and the Bates number(s) of all material that it believes contains the inadvertently disclosed information.

26. If a production contains information that the receiving Party believes is privileged or protected and was inadvertently produced, it will promptly notify the producing Party and provide the Bates number(s) of the item it believes was inadvertently produced. Within 14 days after receiving notification, the producing Party may make a written request for return of the material. If the producing Party does not send a written request for return of the material to the receiving Party within 14 days, the producing Party waives all claims of privilege or protection as to the material, but this still does not operate as a subject matter waiver.

27. When the receiving Party receives a written demand for return of the material, it will make reasonable, good faith efforts to promptly sequester, return or destroy all inadvertently produced material identified by the producing party. If copies of inadvertently produced materials are located or stored on the receiving Party’s Backup System(s), those copies need not be affirmatively removed but, rather, the receiving Party may overwrite those copies according to its normal records management procedures.

28. If the receiving Party must destroy or delete production media (*i.e.*, CD, DVD, thumb drive, or downloaded FTP or JEFS delivery) in order to destroy or delete inadvertently produced material, the producing Party will provide a duplicate copy of the production media

minus only the inadvertently produced material within 14 days of its written request for return of the material to the receiving Party.

29. If the receiving Party intends to challenge the claim of privilege or protection or the inadvertence of the production, it will keep one copy of the inadvertently produced material in a sealed envelope or a sequestered location while seeking a ruling from the Court. Nothing in this Stipulation prevents access by a receiving Party's information technology or security personnel from accessing, in the normal course of their work, systems or locations where inadvertently produced material is sequestered.

Appendix A – Metadata Fields

Field Name	Field Description
Custodian	Name of custodian(s) of email(s) or file(s) produced (Last Name, First Name format) as available
Duplicate Custodian (only if global deduplication applied)	Name of duplicate custodian(s) of email(s) or file(s) produced
BegBates	Beginning Bates# (including Prefix)
EndBates	Ending Bates# (including Prefix)
BegAttach	Beginning Bates number of the first document in an attachment range (only in emails with attachments)
EndAttach	Ending Bates number of the last document in attachment range (only in emails with attachments)
From	From field extracted from an email message
Author	Author field extracted from the metadata of a non-email document
To	To or Recipient extracted from an email message
Cc	Carbon Copy (“Cc”) field extracted from an email message
Bcc	Blind Carbon Copy (“Bcc”) field extracted from an email message
EmailSubject	Subject line extracted from an email message
Filename	File name — Original name of file as appeared in original location
Title	Title field extracted from the metadata of a non-email document
DateSent	Sent date of an email message (mm/dd/yyyy format) (a given email will have either a DateSent or Date Recvd, but not both)
DateRcvd	Received date of an email message (mm/dd/yyyy format) (a given email will have either a DateSent or Date Recvd, but not both)

Field Name	Field Description
DateCreated	Date that a non-email file was created (mm/dd/yyyy format)
DateLastModified	The application recorded time on which the document was last modified
TimeSent	Time e-mail was sent (hh:mm:ss format) (a given email will have either a TimeSent or Time Recvd, but not both)
TimeRcvd	Time e-mail was received (hh:mm:ss format) (a given email will have either a TimeSent or Time Recvd, but not both)
File Extension	File extension of a document
File Path	File path storage location of the document or email if the source application allows for the creation of folders
Native Link	Relative path to any files produced in native format
Text Link	Relative path to any OCR/extracted text files in the production set
Hash Value	MD5 or SHA-1 hash value used to deduplicate the data
Confidentiality Designation	Confidentiality Designation of the document, if any

Dated: June 16, 2021

Agreed to by the parties as follows:

s/ Brook Long
Lawrence Desideri
Brook Long
Winston & Strawn LLP
35 West Wacker Drive
Chicago, IL 60601
Email: LDesideri@winston.com
Email: BLong@winston.com

Counsel for Defendant Village of Hinsdale

JOHN R. LAUSCH JR.
United States Attorney
Northern District of Illinois

s/ Patrick Johnson
PATRICK JOHNSON
KATHLEEN FLANNERY
Assistant United States Attorneys
United States Attorney's Office
Northern District of Illinois
219 South Dearborn Street, Fifth Floor
Chicago, IL 60604
Tel: (312) 353-5327
Email: Kathleen.Flannery@usdoj.gov
Email: Patrick.Johnson2@usdoj.gov

Counsel for Plaintiff United States of America

s/ Sarah Jane Hunt
Sarah Jane Hunt
Thomas E. Kennedy, III
Kennedy Hunt P.C.
906 Olive Street, Suite 200
Saint Louis, MO 63101
Email: sarahjane@kennedyhuntlaw.com
Email: tkennedy@kennedyhuntlaw.com

s/ Brad Staubus
Bradley K. Staubus
Esposito & Staubus LLP
7055 Veterans Boulevard, Unit B
Burr Ridge, IL 60527
Email: bks@eslaw500.com

Counsel for Plaintiff
Trinity Sober Living, LLC

KRISTEN CLARKE
Assistant Attorney General
Civil Rights Division

s/ Max Lapertosa
SAMEENA SHINA MAJEED
Chief
TIMOTHY MORAN
Deputy Chief
MAX LAPERTOSA
Attorney
United States Department of Justice
Housing and Civil Enforcement Section
Civil Rights Division
950 Pennsylvania Avenue NW – 4CON
Washington, DC 20530
Tel: (202) 305-1077
Fax: (202) 514-1116
Email: Max.Lapertosa@usdoj.gov

SO ORDERED this 14 day of July, 2021.


UNITED STATES MAGISTRATE JUDGE